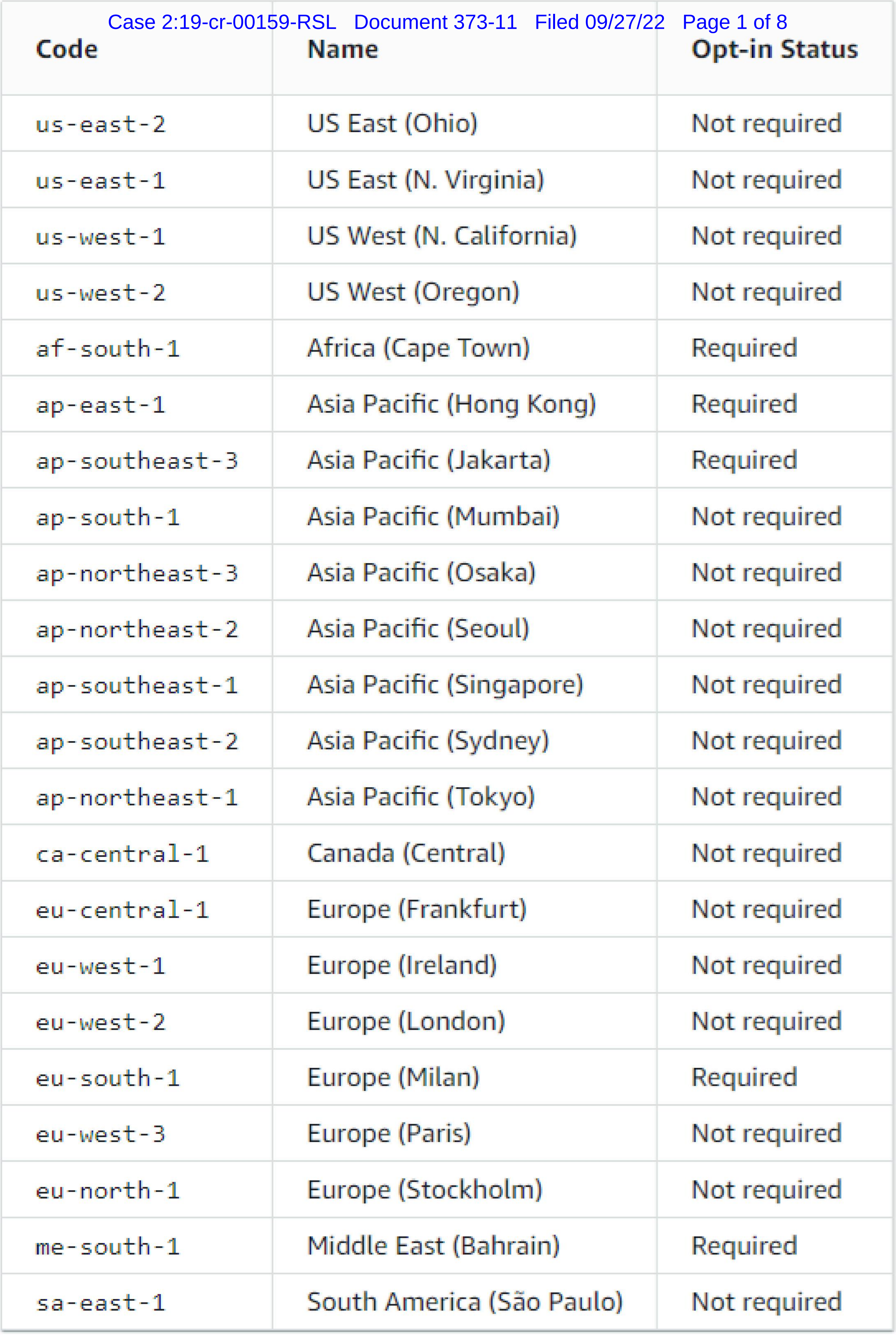
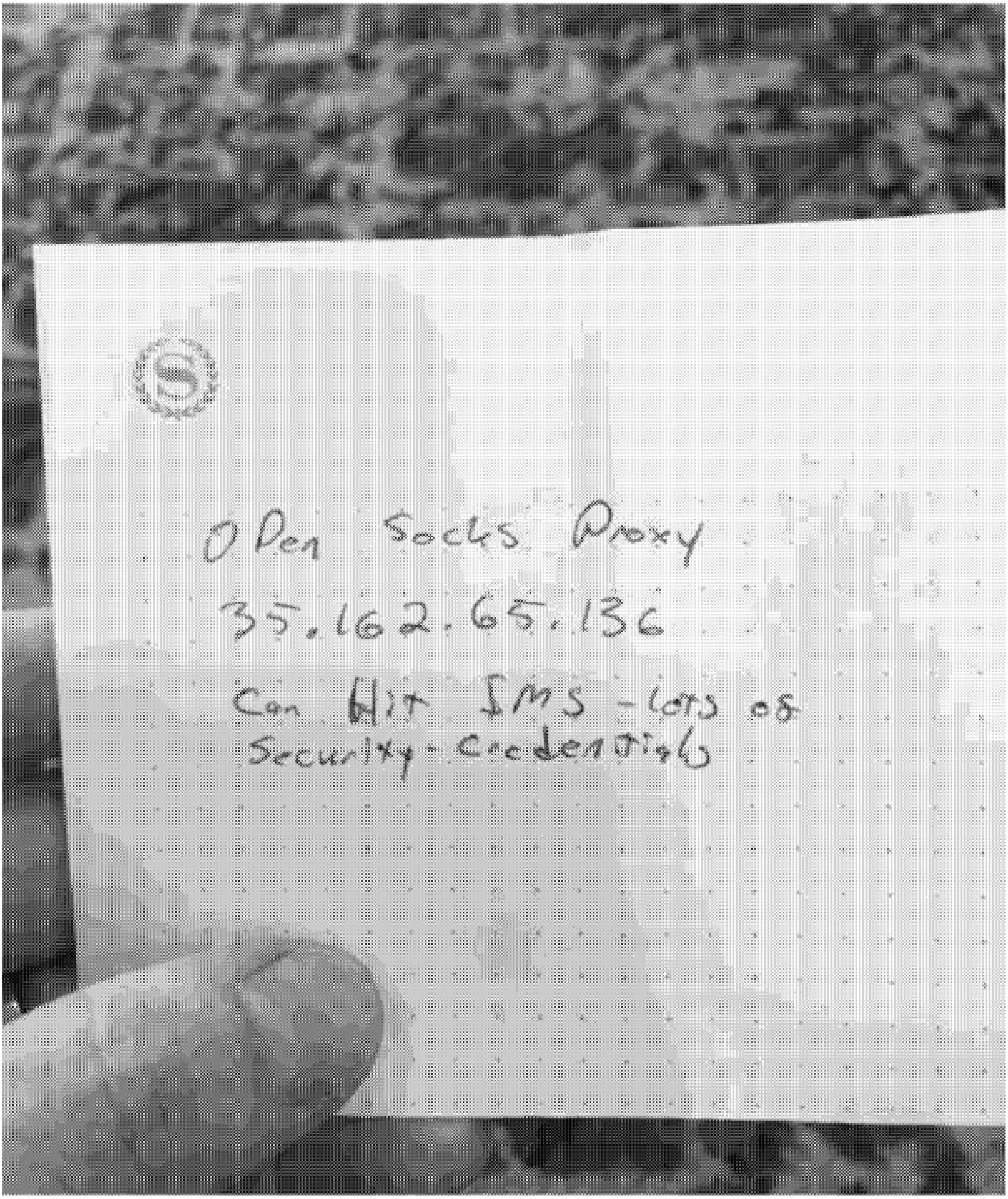


Code	Name	Opt-in Status
us-east-2	US East (Ohio)	Not required
us-east-1	US East (N. Virginia)	Not required
us-west-1	US West (N. California)	Not required
us-west-2	US West (Oregon)	Not required
af-south-1	Africa (Cape Town)	Required
ap-east-1	Asia Pacific (Hong Kong)	Required
ap-southeast-3	Asia Pacific (Jakarta)	Required
ap-south-1	Asia Pacific (Mumbai)	Not required
ap-northeast-3	Asia Pacific (Osaka)	Not required
ap-northeast-2	Asia Pacific (Seoul)	Not required
ap-southeast-1	Asia Pacific (Singapore)	Not required
ap-southeast-2	Asia Pacific (Sydney)	Not required
ap-northeast-1	Asia Pacific (Tokyo)	Not required
ca-central-1	Canada (Central)	Not required
eu-central-1	Europe (Frankfurt)	Not required
eu-west-1	Europe (Ireland)	Not required
eu-west-2	Europe (London)	Not required
eu-south-1	Europe (Milan)	Required
eu-west-3	Europe (Paris)	Not required
eu-north-1	Europe (Stockholm)	Not required
me-south-1	Middle East (Bahrain)	Required
sa-east-1	South America (São Paulo)	Not required

U.S. v. Paige Thompson
CR19-159 RSL
Plaintiff's Exhibit No. 913
Admitted_______________________



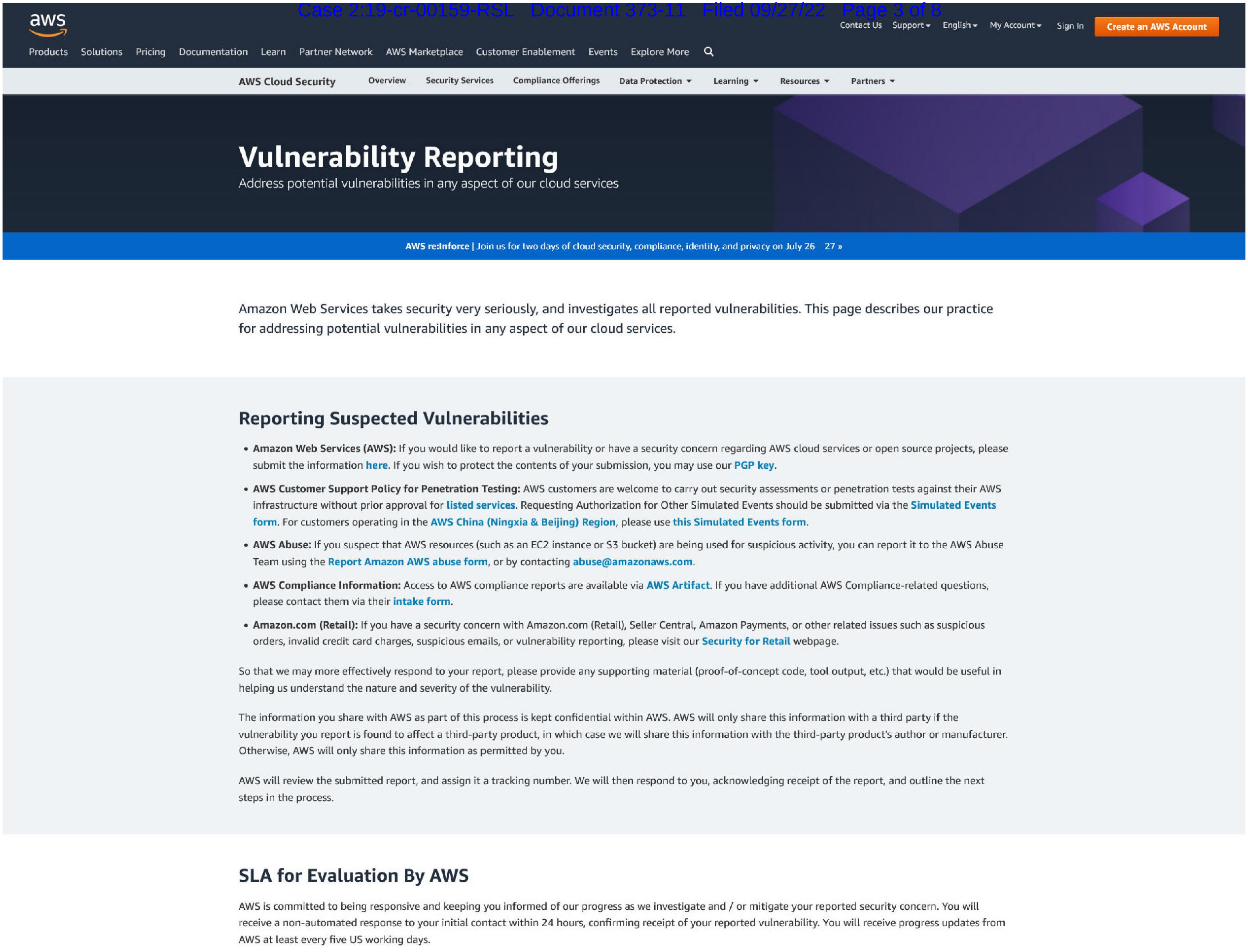
Open Socks Proxy

35.162.65.136

Can Hit IMS - lots of

Security - Credentials

U.S. v. Paige Thompson
CR19-159 RSL
Plaintiff's Exhibit No. 952
Admitted____________________



Vulnerability Reporting

Address potential vulnerabilities in any aspect of our cloud services

AWS re:Inforce | Join us for two days of cloud security, compliance, identity, and privacy on July 26 – 27 »

Amazon Web Services takes security very seriously, and investigates all reported vulnerabilities. This page describes our practice for addressing potential vulnerabilities in any aspect of our cloud services.

Reporting Suspected Vulnerabilities

- **Amazon Web Services (AWS):** If you would like to report a vulnerability or have a security concern regarding AWS cloud services or open source projects, please submit the information **here**. If you wish to protect the contents of your submission, you may use our **PGP key**.
- **AWS Customer Support Policy for Penetration Testing:** AWS customers are welcome to carry out security assessments or penetration tests against their AWS infrastructure without prior approval for **listed services**. Requesting Authorization for Other Simulated Events should be submitted via the **Simulated Events form**. For customers operating in the **AWS China (Ningxia & Beijing) Region**, please use **this Simulated Events form**.
- **AWS Abuse:** If you suspect that AWS resources (such as an EC2 instance or S3 bucket) are being used for suspicious activity, you can report it to the AWS Abuse Team using the **Report Amazon AWS abuse form**, or by contacting **abuse@amazonaws.com**.
- **AWS Compliance Information:** Access to AWS compliance reports are available via **AWS Artifact**. If you have additional AWS Compliance-related questions, please contact them via their **intake form**.
- **Amazon.com (Retail):** If you have a security concern with Amazon.com (Retail), Seller Central, Amazon Payments, or other related issues such as suspicious orders, invalid credit card charges, suspicious emails, or vulnerability reporting, please visit our **Security for Retail** webpage.

So that we may more effectively respond to your report, please provide any supporting material (proof-of-concept code, tool output, etc.) that would be useful in helping us understand the nature and severity of the vulnerability.

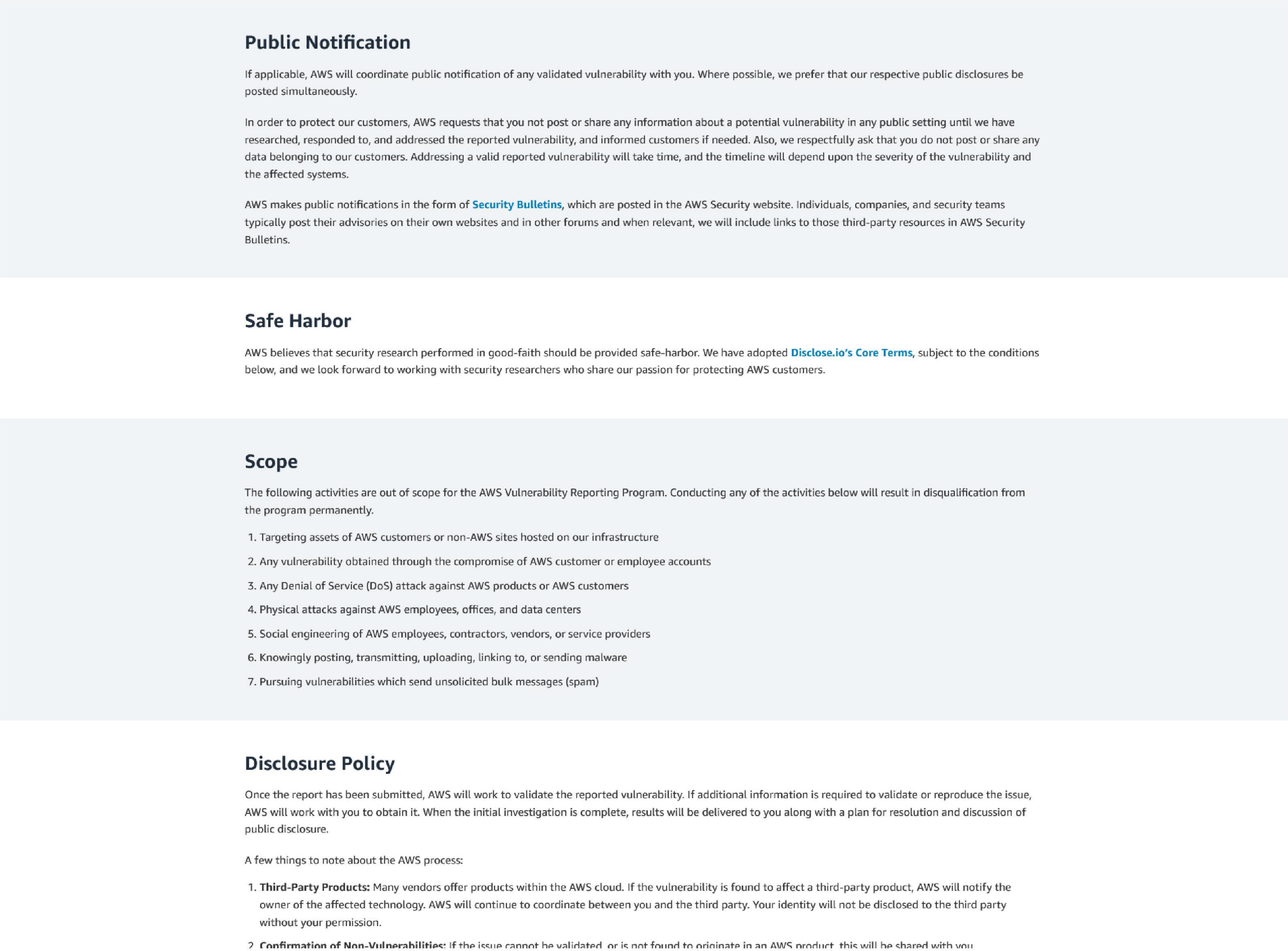
The information you share with AWS as part of this process is kept confidential within AWS. AWS will only share this information with a third party if the vulnerability you report is found to affect a third-party product, in which case we will share this information with the third-party product's author or manufacturer. Otherwise, AWS will only share this information as permitted by you.

AWS will review the submitted report, and assign it a tracking number. We will then respond to you, acknowledging receipt of the report, and outline the next steps in the process.

SLA for Evaluation By AWS

AWS is committed to being responsive and keeping you informed of our progress as we investigate and / or mitigate your reported security concern. You will receive a non-automated response to your initial contact within 24 hours, confirming receipt of your reported vulnerability. You will receive progress updates from AWS at least every five US working days.

U.S. v. Paige Thompson
CR19-159 RSL
Plaintiff's Exhibit No. 954
Admitted__________________



Public Notification

If applicable, AWS will coordinate public notification of any validated vulnerability with you. Where possible, we prefer that our respective public disclosures be posted simultaneously.

In order to protect our customers, AWS requests that you not post or share any information about a potential vulnerability in any public setting until we have researched, responded to, and addressed the reported vulnerability, and informed customers if needed. Also, we respectfully ask that you do not post or share any data belonging to our customers. Addressing a valid reported vulnerability will take time, and the timeline will depend upon the severity of the vulnerability and the affected systems.

AWS makes public notifications in the form of **Security Bulletins**, which are posted in the AWS Security website. Individuals, companies, and security teams typically post their advisories on their own websites and in other forums and when relevant, we will include links to those third-party resources in AWS Security Bulletins.

Safe Harbor

AWS believes that security research performed in good-faith should be provided safe-harbor. We have adopted **Disclose.io's Core Terms**, subject to the conditions below, and we look forward to working with security researchers who share our passion for protecting AWS customers.

Scope

The following activities are out of scope for the AWS Vulnerability Reporting Program. Conducting any of the activities below will result in disqualification from the program permanently.

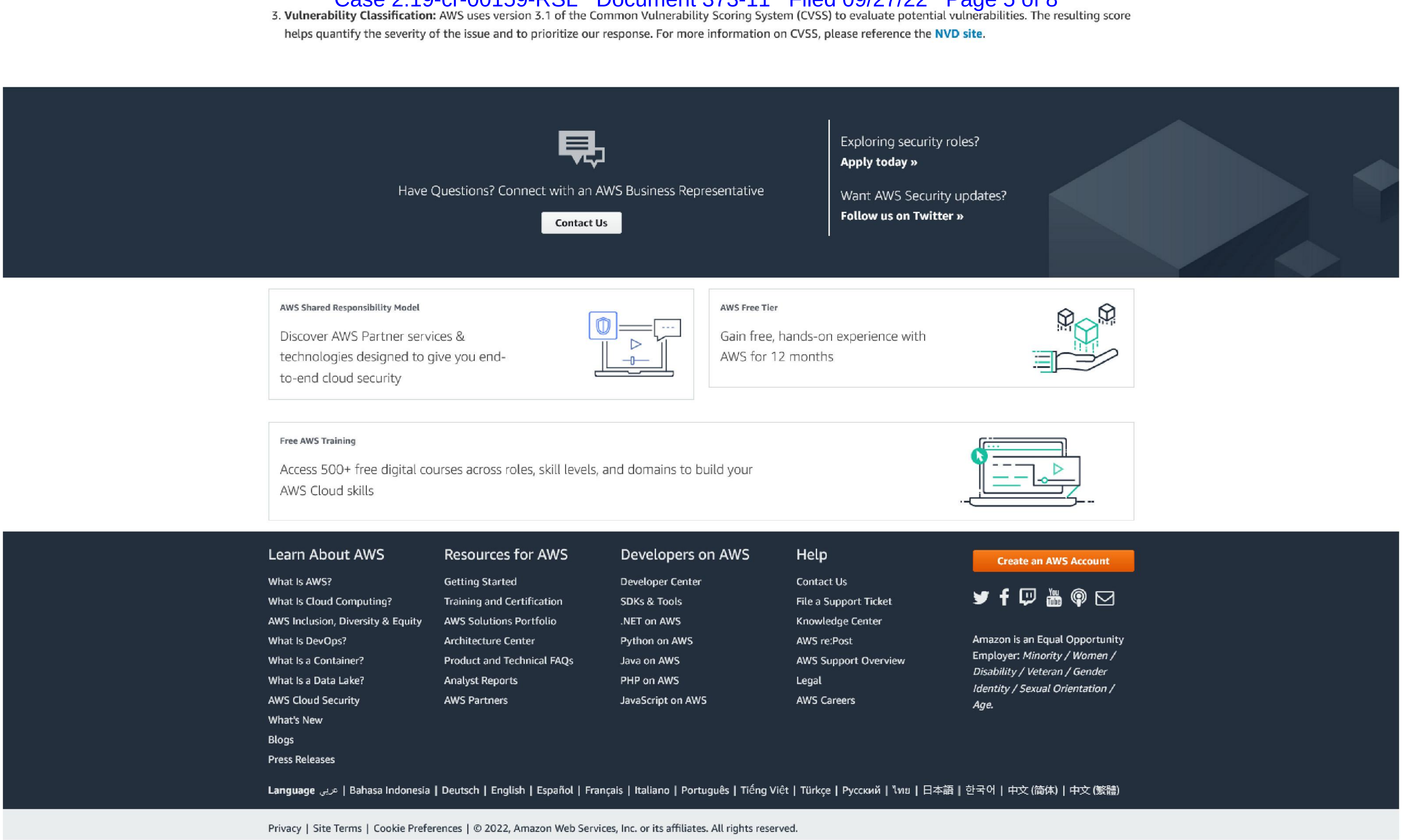
1. Targeting assets of AWS customers or non-AWS sites hosted on our infrastructure
2. Any vulnerability obtained through the compromise of AWS customer or employee accounts
3. Any Denial of Service (DoS) attack against AWS products or AWS customers
4. Physical attacks against AWS employees, offices, and data centers
5. Social engineering of AWS employees, contractors, vendors, or service providers
6. Knowingly posting, transmitting, uploading, linking to, or sending malware
7. Pursuing vulnerabilities which send unsolicited bulk messages (spam)

Disclosure Policy

Once the report has been submitted, AWS will work to validate the reported vulnerability. If additional information is required to validate or reproduce the issue, AWS will work with you to obtain it. When the initial investigation is complete, results will be delivered to you along with a plan for resolution and discussion of public disclosure.

A few things to note about the AWS process:

1. **Third-Party Products:** Many vendors offer products within the AWS cloud. If the vulnerability is found to affect a third-party product, AWS will notify the owner of the affected technology. AWS will continue to coordinate between you and the third party. Your identity will not be disclosed to the third party without your permission.
2. **Confirmation of Non-Vulnerabilities:** If the issue cannot be validated, or is not found to originate in an AWS product, this will be shared with you



3. **Vulnerability Classification:** AWS uses version 3.1 of the Common Vulnerability Scoring System (CVSS) to evaluate potential vulnerabilities. The resulting score helps quantify the severity of the issue and to prioritize our response. For more information on CVSS, please reference the **NVD site**.

Have Questions? Connect with an AWS Business Representative

Contact Us

Exploring security roles?
Apply today »

Want AWS Security updates?
Follow us on Twitter »

AWS Shared Responsibility Model

Discover AWS Partner services & technologies designed to give you end-to-end cloud security

AWS Free Tier

Gain free, hands-on experience with AWS for 12 months

Free AWS Training

Access 500+ free digital courses across roles, skill levels, and domains to build your AWS Cloud skills

Learn About AWS
- What Is AWS?
- What Is Cloud Computing?
- AWS Inclusion, Diversity & Equity
- What Is DevOps?
- What Is a Container?
- What Is a Data Lake?
- AWS Cloud Security
- What's New
- Blogs
- Press Releases

Resources for AWS
- Getting Started
- Training and Certification
- AWS Solutions Portfolio
- Architecture Center
- Product and Technical FAQs
- Analyst Reports
- AWS Partners

Developers on AWS
- Developer Center
- SDKs & Tools
- .NET on AWS
- Python on AWS
- Java on AWS
- PHP on AWS
- JavaScript on AWS

Help
- Contact Us
- File a Support Ticket
- Knowledge Center
- AWS re:Post
- AWS Support Overview
- Legal
- AWS Careers

Create an AWS Account

Amazon is an Equal Opportunity Employer: *Minority / Women / Disability / Veteran / Gender Identity / Sexual Orientation / Age.*

Language عربي | Bahasa Indonesia | Deutsch | English | Español | Français | Italiano | Português | Tiếng Việt | Türkçe | Русский | ไทย | 日本語 | 한국어 | 中文 (简体) | 中文 (繁體)

Privacy | Site Terms | Cookie Preferences | © 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

The Honorable Judge Robert S. Lasnik

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA, Plaintiff, v. PAIGE A. THOMPSON, Defendant.	NO. CR19-159 RSL **STIPULATION REGARDING CELL PHONE IMAGE**

The United States of America, by and through Nicholas W. Brown, United States Attorney for the Western District of Washington, and Andrew C. Friedman, Jessica M. Manca, and Tania M. Culbertson, Assistant United States Attorneys, and the defendant, Paige A. Thompson, and her attorneys, Mohammad A. Hamoudi, Christopher Sanders, Nancy Tenney, Brian Klein, and Melissa Meister stipulate to the following:

1. The FBI seized an Apple iPhone model A1905 (iPhone 8) from Paige Thompson's bedroom on July 29, 2019 and assigned the item evidence number 1B3.

2. John Powers works for the FBI analyzing cellular telephones. Using forensic software, Powers processed the Apple iPhone 8 (1B3) and provided a true and correct image of the phone's contents to FBI Special Agent Joel Martini for his review.

U.S. v. Paige Thompson
CR19-159 RSL
Plaintiff's Exhibit No. 955
Admitted________________

The parties stipulate and agree that no further testimony is necessary to prove that the image of evidence number 1B3 that Special Agent Martini reviewed is a true and correct image of what was recovered from a phone seized by the FBI from Ms. Thompson's bedroom. To be clear, this Stipulation means only that the image is an accurate representation of the phone's contents. There is no agreement as to the truth of the content of any statements contained in evidence number 1B3 or the weight to be given to them.

This Stipulation shall be read to the jury in lieu of having a witness testify as to the source and validity of the exhibit and may then be admitted into evidence and provided to the jury as an Exhibit.

DATED: this 8th day of June, 2022.

s/ Paige A. Thompson
PAIGE A, THOMPSON
Defendant

s/ Mohammad A. Hamoudi
MOHAMMAD A. HAMOUDI
Counsel for Defendant

s/ Christopher Sanders
CHRISTOPHER SANDERS
Counsel for Defendant

s/ Nancy Tenney
NANCY TENNEY
Counsel for Defendant

s/ Brian Klein
BRIAN KLEIN
Counsel for Defendant

s/ Melissa Meister
MELISSA MEISTER
Counsel for Defendant

s/ Andrew C. Friedman
ANDREW C. FRIEDMAN
Assistant United States Attorney

s/ Jessica M. Manca
JESSICA M. MANCA
Assistant United States Attorney

s/ Tania M. Culbertson
TANIA M. CULBERTSON
Assistant United States Attorney